Statement of Howard A. Schmidt,

President & CEO

R & H Security Consulting LLC

Testimony before the House Committee on Energy and Commerce

Hearing on Combating Spyware

January 26, 2005

Chairman Barton, Ranking Member Dingell, and Members of the Committee: My name is Howard A. Schmidt and I am President & CEO of R & H Security Consulting LLC. Over the past 20 years I have served as a Computer Crime Investigator, with the Chandler Arizona Police Department, led the computer exploitation team for the FBI at the National Drug Intelligence Center as well as the Director of Computer Crime and Information Warfare at Air Force Office Special Investigations. I have also been the Chief Security Officer for the Microsoft Corporation and Chief Information Security Officer and Chief Security Strategist for eBay Inc. In the aftermath of 9/11, I was appointed by President Bush as the Vice Chairman of the President's Critical Infrastructure Protection Board and Special Advisor for Cyber Security.

I want to thank you for the opportunity to share with the Committee my perspective on the impact of Spyware – an issue on which this Committee has shown great leadership by working tirelessly to raise public awareness of the potential threat posed by Spyware and by drafting legislation that is carefully targeted to address the bad behavior at the root of the problem, without unnecessarily impacting legitimate software applications. As citizens, we owe a debt of gratitude to Chairman Barton, Representatives Stearns and Schakowsky, the Chairman and Ranking Member, respectively, of the Commerce, Trade, and Consumer Protection Subcommittee, and Representatives Bono and Towns, the

lead Republican and Democrat sponsors of H.R. 29, the SPY ACT. Your willingness to work closely with the private and public sector makes your contribution to this issue even more valuable.

During my previous testimony before House Committees, I have discussed the implications of cyber security on our day to day lives and the protection of critical infrastructure. Today, I would like to tell you why the threats proposed by Spyware threaten more than just our privacy and protection of personal information, but also speak briefly as to the progress that market forces and the private sector have made in the past year. It has been proven time and time again, the tremendous value that results when the public and private sectors work together to protect innovation as well as to improve end user protection.

A. Spyware continues to be a threat to cyber security.

As Chairman Barton discussed in the previous hearing, Spyware represents an intrusion into our day-to-day computing experience without our knowledge. I would like to focus my testimony in two very similar areas, the "end user/consumer" and the enterprise. Other witnesses in previous testimony, as well as today's testimony, have described what Spyware is and some of it's effects, so I will not delve into what Spyware is and how it works again I do not have to go much further then my own family to see first hand the impact Spyware has on the online experience. While my son is a computer crime detective and my wife

teaches computer forensics to law enforcement, the technology expertise stops there. My first example was when my brother-in-law was not able to use his computer for anything because a piece of Spyware had hijacked his browser. Normally it would have been just a matter of resetting the "home page" to the page one would prefer, but this piece of Spyware was so invasive that even using programs specifically designed to remove this application did not function and eventually resulted in his system not functioning at all. He had to send the computer to me in another state and I had to rebuild the entire system.

The second personal example is the PC of my 88 year old father, who uses the PC and the internet for daily entertainment, communications with friends and digital photography. Within a short period of time of him purchasing his new computer, it went from being a high-speed piece of technology to something akin to a 15-year-old computer running so slow it was almost useless. I am sure that these examples are nothing new to many of us in the IT/Security business, but to "normal" users this is very troubling.

To deal with this, industry, using market forces, has responded rapidly to deal with the intrusiveness of Spyware. It started with pop-up blockers being made available for free and then anti-virus vendors started to include anti-Spyware technology into their "security suites." We now have many "toolbars" that have built in pop-up and spy protection. Recently, Microsoft has launched a

Spyware product that is in beta form that shows tremendous promise in providing a technology solution to dealing with a large part of the problem.

As we continue to work on the problem of Spyware, we need to remember that much of the benefits we derive from the online experience is based on the interactive nature of the internet. In the early days of internet use, people interacted with computers. However, in the recent past it has become more of an issue of computers interacting with other *computers* on behalf of people. Although there are those that would exploit computer-to-computer interaction, we should be very sensitive as to not disrupt the legitimate interactive nature of computers acting on behalf of people.

The key difference, as this Committee has learned by working well with the private sector, between good and bad software is not the means by which it is distributed, but the intent and the behavior of the software. As we move towards a computing environment where we develop self-healing, self-repairing, and self-configuring computers, we must ensure the need to, without end-user intervention, have the ability to download upgrades, security fixes, and protective software. Clearly this type of software installation should not and would not fit into the category as Spyware. A classic example is the use of anti-fraud/id theft software updates, these installations are very important to the integrity of the experience on the internet., The concern that many of us have is when the software is introduced

in a deceptive manner and performs functions that are annoying or harmful and difficult, if not impossible, to remove.

At the same time that we are discussing the benefits of convergence of modern day technology, there is also a negative convergence of "traditional" hacking, identity theft, key loggers, and "bots" being installed using what we traditionally call Spyware.

While the vast majority of these acts are covered by provisions of Title 18, Title 5, Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act, the FTC's existing authority to pursue unfair or deceptive trade practices, or international law, H.R. 29, the SPY Act, makes an important contribution to supplementing these laws, and I believe will be successful to the extent that it targets a set of behaviors and not a class of technology. This bill should continue to protect interactive software that is used for positive purposes including where the users have agreed to an end user license agreements (EULA) and understands what their choices are. In short, the end users should be empowered to make their own choices on how they interact with software applications as "one size does not fit all." As many of us said when dealing with many issues of cyber security, we agree that there are four major steps that must be taken to protect end users.

First, the uses of technology and market forces are the strongest

potential solution when it comes to dealing with online threats. As I testified earlier, industry has developed a number of technologies to combat not only Spyware but other threats. Industry's efforts are to be commended and these efforts work for the vast majority of the routine cases we face today. Thanks to freely available anti-Spyware software, including the new Microsoft anti-Spyware beta application, my father's computer is now Spyware free and all indications suggest that it will stay that way.

Second, the education and awareness of ALL users is vital to reducing problems associated with many of the internet threats, whether it is "Phishing," virus and Trojans or Spyware, an educated and informed public is one of the best weapons. Many companies have created "Security Centers" on their web sites to better educate their users as to how protect their computers and their privacy. The National Cyber Security Alliance (NCSA) has consumer tips on its website http://www.stafesafeonline.info. Additional information can be found at http://www.personalfirewallday.org, which provides information for users. The FTC has been a leader in the awareness and education about online security.

Third, companies, even competitors, are working closely together to identify new threats, share information with each other and publish updates to deal with new threats faster than ever in the past. Online companies now are providing free anti-virus services, pop up blockers, and anti-Spyware applications to their

customers. Additionally, many of the industry leaders in identity management such as RSA, Verisign, Entrust and Geotrust are providing tools to improve 2 factor authentication to protect privacy and identity. The National Cyber Security Partnership has brought together leaders in this space across various sectors to better coordinate and publicize the industry and government accomplishments.

Fourth, as with many other issues harming society, technology, education and information are not 100% effective in solving problems To that end, the need to have penalties and trained, equipped and staffed law enforcement personnel to enforce those penalties are essential. While online safety continues to improve day-by-day, hour-by-hour the work of this Committee is beneficial to help us get closer to the 100% level.

The provisions of the SPY ACT should continue to encourage companies to develop and distribute ever more effective and powerful anti-Spyware and security technologies. I look forward to continuing our great working relationship with Congress to ensure that the legislation achieves its aims of protecting and empowering consumers to control their computer systems and to exercise valuable protective measures which fit their situation.

I again would like to thank the Committee for your leadership and attention to the Spyware problem and for extending the invitation for me to appear before you to share my experiences with you today and as in the future as this process

evolves. Cyber security has always and always will employed using a "layered defense" perspective. By working with this body, technology companies, law enforcement agencies, and diplomatic leaders, I believe we can continue to reduce the impact that bad actors have on our online experience and we can continue to strengthen national security, public safety, and economic advancements, while providing for a rich and robust online experience for us all.

I thank you again for the ability to appear here before you today and I look forward to any questions that you may have.

Curriculum Vitae of Howard A. Schmidt CISSP, CISM

Mr. Howard A. Schmidt joined eBay as Vice President and Chief Information Security Officer in May of 2003. In November of 2004 he assumed the role of Chief Security Strategist for eBay, he also assumed the position of Chief Security Strategist for the US CERT Partners Program.

He retired from the White House after 31 years of public service. He was appointed by President Bush as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House in December 2001. He assumed the role as the Chair in January 2003 until his retirement in May 2003.

Prior to the White House, Howard was chief security officer for Microsoft Corp., where his duties included CISO, CSO and forming and directing the Trustworthy Computing Security Strategies Group.

Before Microsoft, Mr. Schmidt was a supervisory special agent and director of the Air Force Office of Special Investigations (AFOSI) Computer Forensic Lab and Computer Crime and Information Warfare Division. While there, he established the first dedicated computer forensic lab in the government.

Before AFOSI, Mr. Schmidt was with the FBI at the National Drug Intelligence Center, where he headed the Computer Exploitation Team. He is

recognized as one of the pioneers in the field of computer forensics and computer evidence collection. Before working at the FBI, Mr. Schmidt was a city police officer from 1983 to 1994 for the Chandler Police Department in Arizona..

Mr. Schmidt served with the U.S. Air Force in various roles from 1967 to 1983, both in active duty and in the civil service. He had served in the Arizona Air National Guard from 1989 until 1998 when he transferred to the U.S. Army Reserves as a Special Agent, Criminal Investigation Division, Computer Crimes Unit, where he continues to serve to this day. He has testified as an expert witness in federal and military courts in the areas of computer crime, computer forensics and Internet crime.

Mr. Schmidt had also served as the international president of the Information Systems Security Association (ISSA) and the first president of the Information Technology Information Sharing and Analysis Center (IT-ISAC). Howard serves on the board of Directors ISC2 the body that provides the ISO certification of the Certified Information Systems Security Professional (CISSP.) He is a former executive board member of the International Organization of Computer Evidence, and served as the co-chairman of the Federal Computer Investigations Committee. He is a member of the American Academy of Forensic Scientists. He serves as an advisory board member for the Technical Research Institute of the National White Collar Crime Center, and was a distinguished

special lecturer at the University of New Haven, Conn., teaching a graduate certificate course in forensic computing.

He served as an augmented member to the President's Committee of Advisors on Science and Technology in the formation of an Institute for Information Infrastructure Protection. He has testified before congressional committees on computer security and cyber crime, and has been instrumental in the creation of public and private partnerships and information-sharing initiatives. He is regularly featured on CNN, ABC, MSNBC, CNBC, Fox TV as well as a number of local media outlets talking about cyber-security.

Mr. Schmidt has been appointed to the Information Security Privacy Advisory Board (ISPAB) to advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST.

Howard holds board positions on a number of corporate boards as well as the BECU board of directors the 5th largest credit union in the country.

Mr. Schmidt holds a bachelor's degree in business administration (BSBA) and a master's degree in organizational management (MAOM) from the

University of Phoenix. He also holds an Honorary Doctorate in Humane Letters.

He is a private pilot and Amateur (HAM) Radio Operator.